

Canada Border  
Services AgencyAgence des services  
frontaliers du Canada

Border Services



Services frontaliers

**Privacy Oversight Committee Meeting /  
Comité de surveillance de la protection des renseignements personnels**

**September 22, 2017/ le 22 septembre 2017**

**RECORD OF DECISION / COMPTE RENDU DES DÉCISIONS**

<b>ATTENDEES / PARTICIPANTS :</b>	Robert Mundie Dan Proulx Pierre Lessard Carl Desmarais (For / Pour Jennifer Lutfallah) Céline Beauregard Karen Haig (For / Pour Claudette Blair) Jean Petitclerc (For / Pour Mélanie Larocque) Hetty Mannethu Anita Andersson (For / Pour Paul Porrior) Sharon Spicer (For / Pour Andrew LeFrank) Stephanie Chénier (For / Pour Lisa Janes) Charles Slowey Robin Lortie
<b>ABSENCES / ABSENTS :</b>	Jim Bissett Erika-Kirsten Easton
<b>CHAIR / PRÉSIDENT :</b>	Robert Mundie
<b>RECORD OF DECISION / COMPTE RENDU :</b>	Robin Lortie

PROTECTION • SERVICE • INTEGRITY



**Item / Point #1 : Opening Remarks / Mots d'ouverture**

**Presenter / Responsable :** Robert Mundie, Chief Privacy Officer / Chef de la protection des renseignements personnels

**Summary of Discussion:**

- The Chief Privacy Officer welcomed the members for their participation at a special meeting focused on *Privacy Act* reforms.

**Sommaire de la discussion :**

- Le chef de la protection des renseignements personnels a accueilli tous les membres pour leur participation à cette réunion spéciale axée sur la réforme de la *Loi sur la protection des renseignements personnels*.

**Item / Point #2 : Renewal of the *Privacy Act* / Réforme de la *Loi sur la protection des renseignements personnels*.**

**Discussion item / Point de discussion**

**Presenters / Responsables :** Robert Mundie

**Summary of Discussion:**

**Annual report of the Office of the Privacy Commissioner:**

- A short summary of the Office of the Privacy Commissioner's (OPC) Annual Report was provided to the members. The points to highlight are:
  - The OPC's report covers the audit on Bill C-51 and the report on Scenario-Based Targeting;
  - The OPC will start to pro-actively launch investigations on subjects of interest rather than focusing all of its attention on complaints;
  - The OPC would like to see penalties / enforcement actions taken for offences committed under the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*.

**Sommaire de la discussion :**

**Rapport annuel du Commissaire à la protection de la vie privée**

- Un court résumé du rapport annuel du Commissaire à la protection de la vie privée (CPVP) est présenté aux membres. Les points à souligner sont les suivants :
  - Le rapport du CPVP aborde la vérification sur le projet de loi C-51 et le rapport sur le ciblage fondé sur des scénarios;
  - Le CPVP commencera à lancer des enquêtes de façon proactive sur les sujets d'intérêt plutôt que de mettre l'accent sur les plaintes;
  - Le CPVP aimerait qu'on impose des amendes ou qu'on prenne des mesures de suivi pour les infractions commises en vertu de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels et les documents électroniques*.



### Renewal of the Privacy Act:

- Some of the suggestions / concerns raised by the members regarding the renewal of the *Privacy Act* are:
  - If order-making powers are provided to the OPC— will they only be applicable to exemptions / exclusions applied on requests, or will they also be applicable to the recommendations provided on PIAs / MOUs / Audits / Reports?;
  - Members would like to see more flexibility in the *Privacy Act* on the data that can be collected / used / shared (e.g. collection of 3<sup>rd</sup> party data / sharing / collecting data from the 5 eyes members, etc.);
  - Members would like a different process regarding the Privacy Impact Assessment / Info Source. The current process is too cumbersome. Members would like to see a process that is more friendly and modern;
  - The renewal of the *Privacy Act* is also an opportunity for the CBSA to see if they would like to review the *Immigration and Refugee Protection Act* as well as the *Custom Act*. (e.g. add to the *Custom Act* a provision that prevents the disclosure of names of intel-officers);
  - The current ETHI recommendations propose that the process for PIAs be a statutory requirement, and that institutions would need to provide a completed PIA up to 90 days prior to implementation of their program. If this becomes the case, it was recommended that the law would also need a legislated timeframe for the OPC to provide its recommendations to the institutions in order that the program not be put on hold pending the recommendations of the OPC.

### Renouvellement de la *Loi sur la protection des renseignements personnels* :

- Voici quelques suggestions/préoccupations des membres au sujet de la réforme de la *Loi sur la protection des renseignements personnels* :
  - Si des pouvoirs exécutoires sont accordés au CPVP, viseront-ils seulement les exemptions/exclusions visant les demandes ou viseront-ils aussi les recommandations au sujet des EFVP/PE/vérifications/rapports?;
  - Les membres voudraient voir plus de souplesse dans la *Loi sur la protection des renseignements personnels* en ce qui concerne les données qui peuvent être recueillies/utilisées/partagée (p. ex. la collecte/le partage de données provenant de tierces parties/la collecte de données provenant de membres du Groupe des cinq, etc.);
  - Les membres aimeraient qu'on adopte un processus différent avec l'évaluation des facteurs relatifs à la vie privée/l'Info Source. Le processus actuel est trop compliqué. Les membres voudraient que le processus soit plus convivial et moderne;
  - La réforme de la *Loi sur la protection des renseignements personnels* est aussi une occasion pour l'ASFC de déterminer si elle souhaite réviser la *Loi sur l'immigration et la protection des réfugiés* ainsi que la *Loi sur les douanes* (p. ex. ajouter dans la *Loi sur les douanes* une disposition qui interdise la divulgation des noms d'agents du renseignement);
  - Selon les recommandations actuelles de l'ETHI, le processus d'EFVP devrait être nécessaire en vertu de la loi et les institutions devraient fournir une EFVP terminée jusqu'à 90 jours avant la mise en œuvre de leur programme. Si cela se produit, on recommande d'imposer des délais prévus par la loi que le CPVP devrait respecter pour la présentation de ses recommandations aux institutions de sorte que le

Border Services



Services frontaliers

- 4 -

<p><b>Follow-up:</b></p> <ul style="list-style-type: none"> <li>The Chief Privacy Officer will send an email soliciting the views / opinions / concerns / recommendations that the members have on each recommendations, in regards to the renewal of the <i>Privacy Act</i>, raised by the ETHI committee.</li> <li>Advice to be prepared on CBSA's position with respect to Privacy Act amendments.</li> </ul>	<p>programme ne soit pas mis en suspens en attendant les recommandations du CPVP.</p> <p><b>Suivi :</b></p> <ul style="list-style-type: none"> <li>Le chef de la protection des renseignements personnels enverra un courriel pour solliciter les points de vue/opinions/préoccupations/recommandations des membres au sujet de chaque recommandation, de la réforme de la <i>Loi sur la protection des renseignements personnels</i> proposé par le comité ETHI.</li> <li>Il faudra se préparer sur la position de l'ASFC au sujet des modifications qui seront apportées à la <i>Loi sur la protection des renseignements personnels</i>.</li> </ul>
<p><b>Item / Point #5 : Round table / Tour de table</b> <b>Presenters / Responsables : All / Tous</b></p>	
<p><b>Summary of Discussion:</b></p> <ul style="list-style-type: none"> <li>No comments and no actions are required.</li> </ul>	<p><b>Sommaire de la discussion :</b></p> <ul style="list-style-type: none"> <li>Aucun commentaire et aucune action ne sont requis.</li> </ul>

Approved by Chair/ Approuvé par le président :

Robert Mundie, Chief Privacy Officer /  
Chef de la protection des  
renseignements personnels

Date / date :

4/10/17



Canada Border  
Services Agency Agence des services  
frontaliers du Canada

Border Services



Services frontaliers

**Privacy Oversight Committee Meeting /  
Comité de surveillance de la protection des renseignements personnels**

**March 09, 2016 / le 09 mars 2016**

**RECORD OF DECISION / COMPTE RENDU DES DISCUSSIONS**

<b>ATTENDEES / PARTICIPANTS:</b>	Robert Mundie Dan Proulx Pierre Giguère Tracy Annett Raymond Bédard (For/pour Denis Vinette) Carl Desmarais (For/pour Lesley L. Soper) Eric Roussin (For/pour Mélanie Larocque) Rob Gilbert Robin Lortie Marie Estabrook Andrew Lawrence Maureen Haley Sharon McKeen	
<b>ABSENCES / ABSENTS:</b>	Lisa Janes Andrew LeFrank Tammy Branch Lisa Fillips Claudette Blair Julie Watkinson Victor Abele France Guèvremont Céline Beauregard Kristine Stolarik	
<b>CHAIR / PRÉSIDENT:</b>	Robert Mundie	
<b>RECORD OF DECISION / COMPTE RENDU:</b>	Robin Lortie	
<b>Item / Point #1: Opening Remarks / Mots d'ouverture</b>		
<b>Presenter / Responsable: Dan Proulx, ATIP Director / Directeur de l'AIPRP</b>		
<b>Summary of Discussion:</b>	<b>Sommaire de la discussion:</b>	
<ul style="list-style-type: none"> <li>The Chief Privacy Officer welcomes and thanks the members for their</li> </ul>	<ul style="list-style-type: none"> <li>Le chef de la protection des renseignements personnels accueille et remercie tous les membres</li> </ul>	

PROTECTION • SERVICE • INTEGRITY

**Canada**



participation.	pour leur participation.
<b>Item / Point #2: Updated and Expanded Information Sharing with Five Country Partners for Immigration Purposes / Mise à jour et expansion du Protocole d'entente pour la mise en commun des renseignements avec nos Partenaires de la Conférence des cinq nations en matière d'immigration</b> <b>Discussion item / Point de discussion</b> <b>Presenters / Responsables: Andrew Lawrence</b>	
<b>Summary of Discussion:</b> <ul style="list-style-type: none"> <li>This presentation was to provide an overview of activities related to the FCC information sharing, sensitize management to some of the risks and challenges identified to date and discuss potential means to address these risks.</li> </ul> <b>Follow-up:</b> <ul style="list-style-type: none"> <li>The Chief Privacy Officer will raise the issue with the Executive Committee that consideration needs to be made on how to ensure a consistent approach to domestic and international information sharing given that the policy areas responsible are found in various directorates and branches within the Agency.</li> </ul>	<b>Sommaire de la discussion:</b> <ul style="list-style-type: none"> <li>Le but de cette présentation était de donner un compte rendu des activités liées à la mise en commun des renseignements de la CCN, à sensibiliser la direction à certains des risques et défis déterminés à ce jour, et à discuter de moyens possibles d'y donner suite.</li> </ul> <b>Suivis :</b> <ul style="list-style-type: none"> <li>Le chef de la protection des renseignements personnels soumettra à l'attention du Comité exécutif la question de la nécessité d'adopter une procédure uniforme d'échange de l'information avec des partenaires canadiens et étrangers, puisque les équipes responsables de la politique se trouvent dans différentes directions et directions générales différentes à l'Agence.</li> </ul>
<b>Item / Point #3: E-Search Policy / Politique sur l'examen des appareils et des supports numériques</b> <b>Presentation item / Point de présentation</b> <b>Presenters / Responsables: Maureen Haley / Sharon McKeen</b>	
<b>Summary of Discussion:</b> <ul style="list-style-type: none"> <li>This presentation was to explain the expansion upon the existing interim policy and clarify authorities and procedures for CBSA officers to follow in the examination of electronic media for the enforcement and investigation of regulatory contraventions or criminal offences supporting the Agency's border</li> </ul>	<b>Sommaire de la discussion:</b> <ul style="list-style-type: none"> <li>Le but de cette présentation était d'expliquer l'expansion de la politique provisoire actuelle et à clarifier les pouvoirs et les procédures à suivre par les agents de l'ASFC lors de l'examen des appareils et des supports numériques aux fins d'exécution de la loi et d'enquête sur les infractions à la réglementation ou les infractions criminelles à l'appui du mandat de l'Agence en matière de</li> </ul>



### legislation mandate.

- This initiative will serve to identify risks and mitigate them on a national scale by ensuring consistent examination, collection, and dissemination practices that respect the personal nature of electronic goods while ensuring the border's security and respect for Canadian law.
- A permanent e-search policy would aim to ensure that examinations of electronic goods are conducted within legal authorities, and that the process is consistent nation-wide.
- The program expect that jurisprudence on this issue will be forthcoming (i.e. Saikaley case), and they are striving to ensure the Agency is well-positioned to defend its authorities.
- Electronic devices and media have been recognized as holding an immense volume of varied personal information; therefore, any data examination or retention must be justified and bear in mind the individual's right to privacy.

### législation frontalière.

- Cette initiative servira à identifier les risques et les atténuer à l'échelle nationale en assurant des pratiques d'examen, de collecte et de diffusion cohérentes qui respectent le caractère personnel des produits électroniques tout en assurant la sécurité des frontières et le respect du droit canadien.
- Une Politique sur l'examen des appareils et des supports numériques permanente aurait pour but d'assurer que les examens de produits électroniques sont menées au sein des autorités légales, et que le processus est conforme à l'échelle nationale.
- Le programme s'attend à ce que la jurisprudence sur cette question est à venir (à savoir le cas Saikaley), et ils s'efforceront de veiller à ce que l'Agence est bien placée pour défendre ses autorités.
- Les appareils électroniques et les médias ont été reconnus comme détenant un immense volume de renseignements personnels variés; par conséquent, tout examen de données ou la rétention doivent être justifiées, et nous devons garder à l'esprit le droit à la vie privée qu'un l'individu possède.

**Item / Point #4:** Bill C-26 – An Act to amend the Criminal Code, the Canada Evidence Act and the Sex Offender Information Registration Act, to enact the High Risk Child Sex Offender Database Act and to make consequential amendments to other Acts / **Projet de loi C-26 -** Loi modifiant le Code criminel, la Loi sur la preuve au Canada et la Loi sur l'enregistrement de renseignements sur les délinquants sexuels, édictant la Loi sur la banque de données concernant les délinquants sexuels à risque élevé (infractions sexuelles visant les enfants) et modifiant d'autres lois en conséquence

**Presentation item / Point de présentation**

**Presenters / Responsable:** Maureen Haley / Sharon McKeen



<p><b>Summary of Discussion:</b></p> <ul style="list-style-type: none"> <li>• This presentation was to provide an overview of the changes in legislation and the impact on the CBSA. <ul style="list-style-type: none"> <li>○ The Government of Canada introduced comprehensive legislation to better address the gravity of sexual offences committed against children. The CBSA will ensure that the use, disclosure and access to the SOIRA information is protected in accordance with the legislation.</li> <li>○ These changes in legislation authorize the CBSA to: <ul style="list-style-type: none"> <li>▪ Receive information from the National Sex Offender Registry (NSOR) regarding High Risk Child Sex Offenders (HRCOS);</li> <li>▪ Identify HRCOS as they re-enter Canada;</li> <li>▪ Collect specific travel information from HRCOS;</li> <li>▪ Disclose collected information to the NSOR in accordance with the <i>Memorandum of Understanding - Establishing an administrative framework for the promotion of cooperation and mutual assistance - between the RCMP and the CBSA</i></li> </ul> </li> </ul> </li> </ul>	<p><b>Sommaire de la discussion:</b></p> <ul style="list-style-type: none"> <li>• Le but de cette présentation était de donner un aperçu des changements à la législation et de l'incidence sur l'ASFC. <ul style="list-style-type: none"> <li>○ Le gouvernement du Canada a présenté une législation complète pour mieux répondre à la gravité des infractions sexuelles commises à l'encontre des enfants. L'ASFC veillera à ce que l'utilisation, la communication et l'accès à l'information reliée à LERDS est protégé conformément à la législation.</li> <li>○ Ces changements dans la législation autorise l'ASFC à: <ul style="list-style-type: none"> <li>▪ Recevoir de l'information à partir du Registre national des délinquants sexuels (RNDS) en ce qui concerne les délinquants sexuels à risque élevé (DSRE);</li> <li>▪ Identifier les DSRE lorsqu'ils entrent au Canada;</li> <li>▪ Recueillir des informations de voyage spécifique aux DSRE;</li> <li>▪ Communiquer les renseignements recueillis du RNDS conformément au Protocole d'entente créant un cadre administratif pour favoriser la coopération et l'aide mutuelle - entre la GRC et l'ASFC.</li> </ul> </li> </ul> </li> </ul>
<p><b>Item / Point #5: Scenarios Based-Targeting / Ciblage fondé sur des scénarios</b>  <b>Presentation item / Point de présentation</b>  <b>Presenters / Responsable: Robert Mundie</b></p>	
<p><b>Summary of Discussion:</b></p> <ul style="list-style-type: none"> <li>• This presentation was to provide an update on the Scenario Based-Targetting, which includes the letter</li> </ul>	<p><b>Sommaire de la discussion:</b></p> <ul style="list-style-type: none"> <li>• Le but de cette présentation était de donner un compte rendu du ciblage fondé sur des scénarios, y compris la lettre qui a été envoyée</li> </ul>

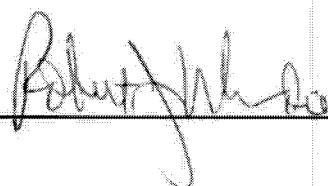




- 5 -

that was sent to the Office of the Privacy Commissioner.	au Commissariat à la protection de la vie privée.
<b>Item / Point #6: Review of the CBSA Privacy Impact Assessment Report / Revue du rapport sur les évaluations des facteurs relatifs à la vie privée qui sont en voie d'élaboration au sein de l'ASFC</b> <b>Presentation item / Point de présentation</b> <b>Presenters / Responsables: Dan Proulx</b>	
<b>Summary of Discussion:</b> <ul style="list-style-type: none"> <li>Update will be provided at the next meeting.</li> </ul>	<b>Sommaire de la discussion:</b> <ul style="list-style-type: none"> <li>Une mise à jour sera transmise à la prochaine réunion.</li> </ul>
<b>Item / Point #7: Round table / Tour de table</b> <b>Presenters / Responsables: All / Tous</b>	
<b>Summary of Discussion:</b> <ul style="list-style-type: none"> <li>No comments and no actions are required.</li> </ul>	<b>Sommaire de la discussion:</b> <ul style="list-style-type: none"> <li>Aucun commentaire et aucune action ne sont requis.</li> </ul>

Approved by Chair/ Approuvé par le président:



Date / date:





Canada Border  
Services Agency

Agence des services  
frontaliers du Canada

Border Services



Services frontaliers

**Privacy Oversight Committee Meeting /  
Comité de surveillance de la protection des renseignements personnels**

**July 5, 2017/ le 5 juillet 2017**

**RECORD OF DECISION / COMPTE RENDU DES DISCUSSIONS**

<b>ATTENDEES / PARTICIPANTS:</b>	Robert Mundie Dan Proulx Ken McCarthy Jim Bisset (For/pour Denis Vinette) Céline Beauregard Marianne Thouin (For/pour Claudette Blair) Johnson Wong (For/pour Mélanie Larocque) Hetty Mannethu Paul Porrior Andrew LeFrank Lisa Janes Blair Bobyk (For/pour Charles Slowey) Gino Lechasseur Jean Bérubé Robin Lortie Neil O'Brien
<b>ABSENCES / ABSENTS:</b>	Jennifer Lutfallah Erika-Kirsten Easton
<b>CHAIR / PRÉSIDENT:</b>	Robert Mundie
<b>RECORD OF DECISION / COMPTE RENDU:</b>	Robin Lortie

PROTECTION • SERVICE • INTEGRITY

**Canada**



Canada Border  
Services Agency

Agence des services  
frontaliers du Canada

Border Services



Services frontaliers

**Item / Point #1: Opening Remarks / Mots d'ouverture**

**Presenter / Responsable:** Robert Mundie, Chief Privacy Officer / Chef de la protection des renseignements personnels

**Summary of Discussion:**

- The Chief Privacy Officer welcomes and thanks the members for their participation.

**Sommaire de la discussion:**

- Le chef de la protection des renseignements personnels accueille et remercie tous les membres pour leur participation.

**Item / Point #2: Enterprise Privacy Architecture - Architecture Vision document / Vision de l'Architecture - Architecture de l'entreprise sur la protection des renseignements personnels.**

**Presentation item / Point de présentation**

**Presenters / Responsables:** Gino Lechasseur / Jean Bérubé

**Summary of Discussion:**

- This presentation provided an overview of the Canada Border Services Agency Enterprise Privacy Architecture Program mandate, vision, expected outcomes activities, the strategic approach and the proposed next steps for this initiative.

**Sommaire de la discussion:**

- Cette présentation a donné un compte rendu du mandat, de la vision, des résultats attendus, de l'approche stratégique et des prochaines étapes proposées liées l'Architecture de l'entreprise sur la protection des renseignements personnels.

**Item / Point #3: Renewal of the Privacy Act and the Access to Information Act / Réforme de la Loi sur la protection sur les renseignements personnels et de la Loi sur l'accès à l'information**

**Presentation item / Point de présentation**

**Presenters / Responsables:** Robert Mundie / Dan Proulx

**Summary of Discussion:**

- Overview of the potential changes in legislation and the possible impacts that these changes may have on the CBSA.

**Follow-up:**

- As part of planned consultations government wide on the *Privacy Act*, President Ossowski has asked the Privacy Oversight Committee to develop

**Sommaire de la discussion:**

- Aperçu des changements potentiels aux législations et de l'incidence que ces changements pourraient avoir sur l'ASFC.

**Suivis :**

- Dans le cadre des consultations planifiées à l'échelle du gouvernement sur la *Loi sur la protection des renseignements personnels*, le président Ossowski a

PROTECTION • SERVICE • INTEGRITY


Canada



- 3 -

<p>a list of issues in terms of implications for the CBSA. A brainstorming session will be organized for late August 2017.</p>	<p>demandé au Comité de surveillance de la protection des renseignements personnels d'élaborer une liste de problèmes en termes d'implications pour l'ASFC. Une séance de remue-méninges sera organisée pour la fin août 2017.</p>
<p><b>Item / Point #4:</b> Review of the CBSA Privacy Impact Assessment Report / Revue du rapport sur les évaluations des facteurs relatifs à la vie privée de l'ASFC.  <b>Presentation item / Point de présentation</b>  <b>Presenters / Responsable:</b> Dan Proulx</p>	
<p><b>Summary of Discussion:</b></p> <ul style="list-style-type: none"> <li>• This presentation provided an overview of the current health of the Privacy Impact Assessments process at the Canada Border Services Agency</li> <li>• Reminder that the new Privacy Impact Assessment Handbook is now available on Atlas.</li> </ul>	<p><b>Sommaire de la discussion:</b></p> <ul style="list-style-type: none"> <li>• Cette présentation a donné un compte rendu de la santé actuelle du processus relié aux Évaluations des facteurs relatifs à la vie privée à l'Agence des services frontaliers du Canada.</li> <li>• Un rappel a également été fourni à tous les membres que le nouveau Manuel d'évaluation des facteurs de confidentialité est maintenant disponible sur Atlas.</li> </ul>
<p><b>Item / Point #5:</b> Round table / Tour de table  <b>Presenters / Responsables:</b> All / Tous</p>	
<p><b>Summary of Discussion:</b></p> <ul style="list-style-type: none"> <li>• No comments and no actions are required.</li> </ul>	<p><b>Sommaire de la discussion:</b></p> <ul style="list-style-type: none"> <li>• Aucun commentaire et aucune action ne sont requis.</li> </ul>

Approved by Chair/ Approuvé par le président:

  
 Robert Mundie, Chief Privacy Officer /  
 Chef de la protection des  
 renseignements personnels

Date / date:

JUL 13 2017



## NOTICE OF DETENTION - AVIS DE RETENUE

Exporter/Importer - Exportateur/Importateur


Detention No. - N° de détention

Other reference No. - Autre n° de référence

CBSA office - Bureau de l'ASFC

Date (YYYY-MM-DD) - Date (AAAA-MM-JJ)

### Part A - Partie A

The goods described below are detained under Section 101 of the *Customs Act*. You are advised that these goods may not be exported from or imported into Canada until a CBSA officer is satisfied that these goods comply with the *Customs Act* and any other Act of Parliament that prohibits, controls, or regulates the exportation or importation of goods, and any regulations made thereunder.

Les marchandises décrites ci-dessous sont détenues en conformité à l'article 101 de la *Loi sur les douanes*. Vous êtes avisé que ces marchandises ne peuvent être exportées du ou importées au Canada sans qu'un agent de l'ASFC soit satisfait que ces marchandises sont en conformité avec la *Loi sur les douanes* et toute autre loi fédérale prohibant, contrôlant et réglementant les exportations ou importations, ainsi qu'à leurs règlements d'application.

Description of goods (specify details and attach documents if available) - Désignation des marchandises (spécifiez les détails et attachez les documents disponibles)

Shipper's reference No. - N° de référence de l'expéditeur

Location of goods - Localisation des marchandises

The goods described above are being detained for the following reasons: - Les marchandises décrites ci-haut sont détenues pour les raisons suivantes :

You are required to contact the following address concerning the requirements that have to be met. - Vous devez communiquer à l'adresse suivante concernant les exigences requises.

CBSA office (name and address) - Bureau de l'ASFC (nom et adresse)

Badge No. - N° d'insigne

Signature of issuing officer - Signature de l'agent

### Part B - Partie B

I acknowledge receipt of this notice - J'accuse réception de cet avis

Signature

Date (YYYY-MM-DD) - Date (AAAA-MM-JJ)

### Part C - Partie C

Disposition of the goods - Dispositions prises à l'égard des marchandises

Document No. - N° du document

Date (YYYY-MM-DD) - Date (AAAA-MM-JJ)



## OPERATIONAL BULLETIN: OBO-2019-055

### TITLE: Implementation of the Policy on Port of Entry (POE) Examinations of Travellers' Digital Devices

<b>Date of Issue:</b> 2019-11-29	<b>Mode(s):</b> All	<b>Target Audience:</b> National	<b>Area of Interest:</b> Port of Entry
-------------------------------------	------------------------	-------------------------------------	---

#### Details:

- The purpose of this Operational Bulletin (OB) is to introduce the CBSA's new policy on POE Examinations Of Travellers' Digital Devices to all staff (Enforcement Manual Part 4 Chapter 16).
- The new policy expands on the previous OB (PRG-2015-31), providing more details on the procedures to be followed by all operational staff.
- The policy will go live on Monday December 2, 2019.
- The policy on POE Examinations Of Travellers' Digital Devices will provide CBSA Officers with a framework for the lawful, reasonable and progressive POE examinations of travellers' digital devices while recognizing and respecting the potential private nature of data contained within these devices.
- This policy applies to any CBSA Officer who may, as part of their duties, examine a traveller's digital device as part of a secondary examination under the *Customs Act* or the *Immigration and Refugee Protection Act* at a port of entry.
- Mandatory training is available and must be completed by all Border Services Officers (BSOs)/Superintendents/Chiefs within 3 months from the issuance of this policy. Training is recommended for anyone else whose work has a nexus to POE examinations of digital devices. (Course code: S7188-P)

#### Roles and Responsibilities:

- Border Services Officers (BSOs) are responsible for:
  - a. BSOs working at POE must be familiar with the policy on the examination of travellers' digital goods.
  - b. BSOs are responsible for taking the mandatory training on the Examination of Digital Devices

- c. BSOs are responsible for following the guidance and directives contained within the policy on the examination of travellers' digital goods.
- d. As per the policy guidance contained herein, BSOs are responsible for:
  - i. remaining sensitive to the potential private nature of data stored on digital devices;
  - ii. following guidance on when and how digital devices can be examined;
  - iii. reporting any examinations of travellers' digital devices to CBSA Headquarters (as per OB PRG-2017-61 and per Shift Briefing Bulletin 2019-HQ-AC-05-10)
  - iv. making timely and comprehensive notes whenever a traveller's digital device is examined.
- Regional Intelligence Officers (RIO) are responsible for:
  - a. Familiarizing themselves with the policy on examinations of travellers' digital devices, and
  - b. Remaining available to consult with other CBSA Officers who may examine travellers' digital goods, including BSOs that encounter lookouts when processing travellers, to provide additional information to the BSO that could assist the BSO in determining if a digital device examination is justified.
- Superintendents are responsible for:
  - a. Familiarizing themselves with the policy on examinations of travellers' digital devices;
  - b. Ensuring BSOs working in the traveller continuum familiarize themselves with the policy on examinations of travellers' digital devices; and
  - c. Ensuring BSOs follow the policy guidance contained herein, including but not limited to:
    - i. Not conducting digital device exams as a matter of course;
    - ii. Not conducting examinations solely for the purpose of finding an offence under the Criminal Code;
    - iii. Taking comprehensive and timely notes when devices are examined;
    - iv. Remaining sensitive to the potential private nature of these goods; and
    - v. Reporting to CBSA HQ all instances of examinations of travellers' digital devices as per PRG-2017-61 and per Shift Briefing Bulletin 2019-HQ-AC-05-10
  - d. Performing periodic compliance verifications to ensure BSOs are following the policies contained herein.
- Chiefs are responsible for:
  - a. Ensuring ports of entry in their jurisdiction are aware of the policy on examinations of travellers' digital goods;
  - b. Ensuring BSOs in their jurisdiction have completed the requisite training on the examination of digital devices;

- c. Ensuring Superintendents exercise due diligence in reporting instances of digital goods examinations to CBSA Headquarters as per PRG-2017-61 and per Shift Briefing Bulletin 2019-HQ-AC-05-10; and
- d. Ensuring Superintendents perform periodic compliance verifications to ensure BSOs are following the policies contained herein, including note taking.

**Contact Information:**

Traveller Compliance Unit, Program Compliance and Outreach Division, Travellers Branch

Questions regarding this bulletin should be directed to the Traveller Compliance Unit via e-mail at:

**Approved by:**

Giovanni Matrisciano, Director Program Compliance and Outreach Division,  
Traveller Programs Directorate, Travellers Branch

**Effective Date:** 2019-12-02

**Updated:** N/A





## BULLETIN OPÉRATIONNEL : OBO-2019-055

### TITRE : Mise en œuvre de la politique sur l'examen des appareils numériques des voyageurs aux points d'entrée (PDE)

<b>Date de publication :</b> 2019-11-29	<b>Mode :</b> Tous	<b>Public cible :</b> National	<b>Secteurs d'intérêt :</b> Points d'entrée
--	-----------------------	-----------------------------------	--

#### Détails :

- Le présent Bulletin opérationnel (BO) a pour objectif de présenter à tout le personnel la nouvelle politique de l'ASFC sur les examens des appareils numériques des voyageurs aux points d'entrée (Manuel d'exécution de l'ASFC, partie 4, chapitre 16).
- La nouvelle politique élargit les lignes directrices du BO précédent PRG-2015-31 en fournissant plus de détails sur les procédures à suivre par tout le personnel opérationnel..
- La nouvelle politique sera mise en œuvre le lundi 2 décembre 2019.
- La politique sur les examens des appareils numériques des voyageurs aux PDE fournira aux agents de l'ASFC un cadre pour les examens légaux, raisonnables et progressifs des appareils numériques des voyageurs aux points d'entrée, tout en reconnaissant et en respectant le caractère potentiellement privé des données contenues dans ces appareils.
- La présente politique s'applique à tout agent de l'ASFC qui peut, dans le cadre de ses fonctions, examiner l'appareil numérique d'un voyageur dans le cadre d'un examen secondaire en vertu de la *Loi sur les douanes* ou de la *Loi sur l'immigration et la protection des réfugiés* (LIPR) à un point d'entrée.
- La formation obligatoire est disponible et doit être complétée par tous les agents des services frontaliers (ASF)/Surintendants/Superviseurs/Chefs des opérations dans les trois mois suivant la publication de la présente politique. La formation est recommandée à toute personne dont le travail a un lien avec les examens de PDE des appareils numériques. (Code du cours: S7188-P)

#### Rôles et responsabilités :

##### Agent des services frontaliers (ASF)

- a. L'agent des services frontaliers (ASF) qui travaille à un PDE doit se familiariser avec la politique sur l'examen des appareils numériques des voyageurs.
- b. L'ASF doit suivre la formation obligatoire sur l'examen des appareils numériques.

- c. L'ASF doit suivre les instructions et les directives de la politique relative à l'examen des appareils numériques des voyageurs.
- d. Conformément aux instructions de la présente politique, l'ASF doit :
  - i. avoir conscience de la nature confidentielle possible des données stockées sur les appareils numériques;
  - ii. suivre les instructions relatives aux circonstances dans lesquelles les appareils numériques peuvent être examinés et au moment de le faire;
  - iii. signaler tout examen de appareils numériques des voyageurs à l'Administration centrale de l'ASFC (selon le BO PRG-2017-61 et selon le Bulletin d'information de quart de travail : 2019-HQ-AC-05-10);
  - iv. prendre des notes exhaustives à point nommé lors de l'examen dudit appareil.

#### Agent régional du renseignement (AAR)

- a. se familiariser avec la politique sur l'examen des appareils numériques des voyageurs;
- b. demeurer disponible pour consulter d'autres agents de l'ASFC qui pourraient examiner les appareils numériques des voyageurs, notamment les ASF qui ont pris connaissance d'un avis de surveillance visant un voyageur pendant le traitement de ce dernier, et ce afin de fournir des renseignements supplémentaires aux ASF pour déterminer si l'examen d'un appareil électronique est justifié.

#### Surintendant/Superviseur

- a. se familiariser avec la politique sur l'examen des appareils numériques des voyageurs;
- b. s'assurer que les ASF qui travaillent dans le continuum des voyageurs se familiarisent avec la politique sur l'examen des appareils numériques des voyageurs;
- c. s'assurer que les ASF suivent les instructions de la présente politique, notamment :
  - i. de ne pas mener d'examens systématiques de appareils numériques;
  - ii. de ne pas effectuer des examens uniquement dans le but de trouver une infraction au Code criminel;
  - iii. de prendre des notes exhaustives à point nommé lors de l'examen d'un dispositif;
  - iv. d'avoir conscience de la nature confidentielle possible stockées sur l'appareil numérique;
  - v. de signaler tout examen desdits appareils numériques à l'Administration centrale de l'ASFC selon PRG-2017-61 et du Bulletin d'information de quart de travail 2019-HQ-AC-05-10
- d. effectuer des vérifications périodiques de la conformité pour s'assurer que les ASF respectent les dispositions de la présente politique.

#### Chef des opérations

- a. s'assurer que toutes les PDE qui relèvent de lui connaissent la politique sur l'examen des appareils numériques des voyageurs;
- b. s'assurer que les ASF qui relèvent de lui ont suivi la formation requise sur l'examen des appareils numériques;

- c. s'assurer que les surintendants/superviseurs font preuve de diligence raisonnable lorsqu'ils signalent les examens des appareils numériques à l'Administration centrale de l'ASFC selon PRG-2017-61 et du Bulletin d'information de quart de travail 2019-HQ-AC-05-10;
- d. veiller à ce que les surintendants/superviseurs effectuent des vérifications périodiques de la conformité afin de s'assurer que les ASF respectent les dispositions de la présente politique, y compris celles relatives à la prise de notes.

**Coordonnées :**

Conformité des voyageurs, Division de la conformité au programme et de la sensibilisation,  
Direction générale des voyageurs

Les questions concernant ce bulletin doivent être adressées à l'Unité de vérification de la conformité des voyageurs par courrier électronique à l'adresse suivante:

**Approuvé par :**

Giovanni Matrisciano, Directeur Division de la conformité au programme et de la sensibilisation,  
Direction des programmes des voyageurs, Direction générale des voyageurs

**Date d'entrée en vigueur :** 2019-12-02

**Mis à jour le :** s.o.



## OPERATIONAL BULLETIN : PRG-2013-30

### TITLE: Clarification of *Criminal Code* s. 495 Arrest Authorities for Enforcement and Intelligence Officers

Date of Issue:	Mode(s)	Target Audience	Areas of Interest
2013/05/31	Non Port of Entry	National Enforcement & Intelligence Division	Inland Enforcement Criminal Investigation Intelligence

#### Details:

#### POLICY STATEMENT

1. The following operational bulletin pertains to **CBSA Inland Enforcement Officers, Regional Intelligence Officers and Criminal Investigators**, hereinafter referred to as Enforcement and Intelligence Officers (**E&I officers**), who routinely conduct their work away from a Port of Entry. The directive confirms their authority to arrest *for Customs Act* (CA) and the *Immigration and Refugee Protection Act* (IRPA) offences.
2. E&I officers take appropriate enforcement actions against individuals who are non-compliant with the IRPA and the CA. These actions may include the investigation, detention and arrest of individuals in relation to offences under the IRPA and the CA.
3. E&I officers, where they are designated under subsection 138(1) of the IRPA or are performing any duty in the administration or enforcement of the CA, are peace officers for the purposes of carrying out their duties in the administration and enforcement of the IRPA and/or the CA as the case may be.
4. E&I officers have the authority under s. 495 of the *Criminal Code of Canada* (CC) to arrest any person who is committing an offence under the IRPA or the CA. It is an offence pursuant to s. 129(1)(d) of the IRPA to obstruct or impede an officer in the performance of the officer's duties under IRPA. It is an offence pursuant to s.153.1 of the CA to hinder an officer from doing anything that the officer is authorized to do under the CA.





- 2 -

## CONSIDERATIONS

5. This bulletin serves as a clarification of existing authorities and powers under the IRPA and CA and should not be considered as a source of any new authority.
6. While the CC is a federal statute, law enforcement and policing in Canada fall under provincial jurisdiction. Federal law enforcement agencies can only enforce the criminal law with express statutory enablement or by agreement with the province (s. 92(14) *Constitution Act of 1867*).
7. As a result, E&I officers are only peace officers for the purpose of administering and enforcing the CA and the IRPA and do not have the authority under s. 495 of the CC to arrest for any CC offences.
8. Where an E&I officer is obstructed, hindered or otherwise interfered with by any person (including a Canadian Citizen) in the performance of the officer's duties under the CA or the IRPA, that officer may exercise his/her authority under s. 495 of the CC to arrest that person for the offence of hindering under s. 153.1 of the CA or for the offence of obstructing or impeding under s. 129(1)(d) of the IRPA, as the case may be.
9. Even where the nature of the obstruction, interference or hindrance is violent in nature and the officer is concerned for their personal safety or the safety of the public, the officer's arrest authorities are in relation to those offences set out in the CA and the IRPA. E&I officers are peace officers for the purposes of enforcing the IRPA and/or the CA. E&I officers are not peace officers for the purposes of enforcing the CC. E&I officers are entitled to and subject to the legal protections and responsibilities involved in arresting for an offence under the CA or under the IRPA, including those applicable to the appropriate use of force to affect such an arrest.
10. When an E&I officer makes an arrest for an offence under s. 129(1)(d) of the IRPA or s. 153.1 of the CA, it is imperative that the person arrested is informed of the reason for their arrest, cautioned regarding their right to silence and informed of their right to counsel, and afforded such rights, as required by the *Canadian Charter of Rights and Freedoms*. Further details regarding arrest procedures are set out in CBSA's Enforcement Manual
11. CBSA Criminal Investigations is responsible for investigating and laying charges for offences under the IRPA and the CA. If a CC offence has occurred, officers shall consider calling the police of jurisdiction so they may investigate.
12. The exercise by E&I officer of powers in the CC which apply to all members of the public (for example those set out in s.494 of the CC) cannot be endorsed



- 3 -

by the CBSA. The use of CBSA assets in such circumstances is not authorized by the CBSA. The Treasury Board's Policy on Legal Assistance and Indemnification, limits the legal assistance and indemnification available to any Crown servant, including an E&I officer, who chooses to act outside the scope of their duties or course of employment.

13. This operational bulletin is effective immediately and corresponding updates will be incorporated into relevant enforcement manuals, operating procedures and training materials.

#### **Contact Information:**

Questions regarding this bulletin should be directed to:

Lynn Lawless  
Director, Program Management Division  
Enforcement and Intelligence Programs  
Programs Branch  
(613)954-9149  
lynn.lawless@cbsa-asfc.gc.ca

#### **Approved by:**

Chris Henderson  
Director General,  
Enforcement & Intelligence Programs  
Programs Branch

**Effective Date:** 2013-05-31

**Updated:** N/A

Additional bulletins:

### **WORKPLACE SCENARIOS - Non Port of Entry Peace Officer CC s. 495 Arrest Authorities for CBSA Enforcement and Intelligence Officers:**

The Programs Management Division has developed the following 8 workplace scenarios to assist E&I officers in understanding Non Port of Entry arrest authorities:



- 4 -



**WORKPLACE SCENARIOS**  
**Non Port of Entry Peace Officer**  
**CC s. 495 Arrest Authorities for CBSA**  
**Enforcement and Intelligence Officers**

May 2013



Canada

**CBSA ASFC**

**CBSA Peace Officers Authorities Scenarios**

**#1 - Hindering / Impeding an Officer**

- An Investigator and his team of five are executing a search warrant as part of a criminal investigation for evasion of duties under the Customs Act. A man and his wife are present in the home while the search is taking place. When the Investigator makes an attempt to search a closet in the basement, the man charges forward and tells the Investigator he can't look in the closet as it contains personal items. The Investigator informs the man that the closet is part of the areas to be searched under the search warrant and that he is authorized to look in the closet. The husband physically blocks the Investigator while the wife grabs the key to the closet door and drops it into a nearby sink. Both are arrested for s. 153.1 of the CA.
- **CBSA Authority:** Arrest under s.495 CC for hindering s.153.1 of the Customs Act.



- 5 -

CBSA ASFC

## CBSA Peace Officers Authorities Scenarios

### #2 - Assault of an Inland Enforcement Officer

- Two Inland Enforcement Officers are attending a park seeking the subject of a warrant for removal. The lead Officer approaches the subject who is seated on a bench. The Officer informs the man that they are CBSA Enforcement Officers and they are there to arrest him. The man's wife, a Canadian Citizen who is close by, runs at the Officers and begins yelling "leave my husband alone" and she begins to punch and kick one of the officers.
- CBSA Authority:** Arrest the man's wife, a Canadian Citizen under s.495 CC for impeding s.129(1)(d) of IRPA.

3

PROTECTION • SERVICE • INTEGRITY

CBSA ASFC

## CBSA Peace Officers Authorities Scenarios

### #3 - Assault of an Investigator/Intelligence Officer

- The Criminal Investigations office is conducting a search of a private business pertaining to misdescribed vitamins which were imported into Canada. Both Criminal Investigators and Intelligence Officers are searching the offices for documents falling within the scope of the warrant issued under s. 111 of the Customs Act. The owner is cooperative with the search and shows the officers to the office area. The owner introduces his employees to the officers. As the officers enter the office, an employee pulls a knife from his pocket and slashes the arm one of the officers.
- CBSA Authority:** Arrest under s. 495 CC for hindering s. 153.1 of the Customs Act.

4

PROTECTION • SERVICE • INTEGRITY





- 6 -

CBSA ASFC

## CBSA Peace Officers Authorities Scenarios

### #4 - Witnessing Significant Criminal Event

- Two CBSA Intelligence officers are leaving the court house and witness a group of girls who appear to be beating someone on the ground. One of the officers immediately calls 911 on his cell phone. There are no police officers visible but several onlookers are watching the beating and two of them are taping the incident with their cell phones. One of the CBSA officers yells "STOP" and the attackers stop assaulting the victim. However, the victim of the beating gets up from the sidewalk and pulls a knife from her coat pocket. Both officers yell at the girl to drop the knife, but instead she puts the knife against the throat of one of her attackers.
- CBSA Authority:** CBSA Officers have no s. 495 peace officer arrest authority to intervene.

5

PROTECTION • SERVICE • INTEGRITY

CBSA ASFC

## CBSA Peace Officers Authorities Scenarios

### #5 - Assisting Other Law Enforcement Agencies – Customs Act

- An Officer is working on a Joint Forces Operation with Police and the RCMP. The information to obtain a Search Warrant states that firearms are alleged to have been smuggled into Canada in contravention of the Customs Act. After entry, the Officer and a local police officer are in the kitchen area along with the house occupant. The man becomes very agitated, grabs the police officer and begins to punch him repeatedly and attempts to disarm the police officer by reaching for his firearm.
- CBSA Authority:** Arrest under s. 495 CC for hindering s. 153.1 of the Customs Act. In this scenario, CBSA officers are lawfully in the dwelling house. The attack on the Police Officer would constitute the hindering of the search of the premises in order to lawfully execute the arrest.

6

PROTECTION • SERVICE • INTEGRITY



- 7 -

CBSA ASFC

## CBSA Peace Officers Authorities Scenarios

### #6 - Assisting Other Law Enforcement Agencies – IRPA

- A search warrant under IRPA is obtained by Criminal Investigations. Inland Enforcement, Criminal Investigations and police attend the business. During room clearing, a police officer is assaulted by someone hiding in a closet.
- **CBSA Authority:** Arrest under s. 495 CC for impeding 129(1)(d) of IRPA. In this scenario, CBSA officers are lawfully in the dwelling house. In order to lawfully execute the arrest, the attack on the Police Officer would need to constitute impeding the search of the premises.

7

PROTECTION • SERVICE • INTEGRITY

CBSA ASFC

## CBSA Peace Officers Authorities Scenarios

### #7 - Assisting Other Law Enforcement Agencies - CDSA & Criminal Code

- A CBSA Intelligence Officer is working on a Joint Forces Operation with the Police. The team is conducting a search of a business. The search warrant lists "drugs/substances controlled by the Controlled Drugs and Substances Act (CDSA) and credit cards and credit card making devices" as items to be searched for. There are no Customs Act or Immigration and Refugee Protection Act offences included in the Information to Obtain a Search Warrant. The owner of the business is sitting at his desk and asks what this is all about. The Police Officer explains the search warrant and provides a copy to the owner. The owner begins yelling at the officers. The Police Officer explains in a calm manner that they will not be leaving and that they are legally authorized to be there and to search the premises for anything under the CDSA, and that they are also searching for credit card making equipment. The man, completely enraged, opens a drawer from his desk and pulls out a handgun.
- **CBSA Authority:** CBSA Officer may only be present if there is a border nexus to their proposed duties. In the scenario described, CBSA Officers should not be present.

8

PROTECTION • SERVICE • INTEGRITY



- 8 -

CBSA ASFC

## CBSA Peace Officers Authorities Scenarios

### #8 Non enforcement duties

- Officers are directed by management to attend a public firing range, rented for their exclusive use to fulfill required firearms practice. On arrival, the uniformed CBSA officers properly identify themselves to persons who are using the facility. However the other patrons are displeased at having to abandon the range because CBSA reserved it. One individual refuses to leave and physically interferes with officers as they attempt to gain access to the range.
- **CBSA Authority:** Presence at a firing range does not equate to the administration or enforcement of the IRPA or CA, as such there are no Peace Officer authorities.

9

PROTECTION • SERVICE • INTEGRITY



## OPERATIONAL BULLETIN: OBO-2020-009

### TITLE: Collection of Data Related to the Examinations of Travellers' Digital Devices: Reporting Requirement in the Integrated Customs System (ICS)

<b>Date of Issue:</b> 2020-01-30	<b>Mode(s):</b> All	<b>Target Audience:</b> BSOs/Superintendents/Chiefs	<b>Area of Interest:</b> National
-------------------------------------	------------------------	--	--------------------------------------

#### **\*\*REPLACES PRG-2017-61\*\***

The purpose of this Operational Bulletin (OB) is to advise of a new mandatory data reporting requirement within the Integrated Customs System (ICS) following any examination of travellers' digital device(s).

#### **Details:**

- Since November 20, 2017, officers have been required to report all instances where the data contained on the digital device(s) of a traveller had been examined.
- Officers are no longer required to report examinations on the digital examination tracking sheet, nor are officers required to record examination data using the Interim Reporting Tool.
- The Integrated Customs System (ICS) has been updated to reflect the potential examinations of electronic device searches. All examinations, resultant and non-resultant, **must** be recorded using ICS following the guidelines below.
- A resultant outcome is defined as a situation whereby the officer has identified, during the examination process, a contravention to the *Customs Act* and/or any other act of Parliament (e.g. *Criminal Code*, *Immigration and Refugee Protection Act*, *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*).
- "Digital device" for the purposes of this policy means mobile phones (cell phones), smartphones, computers, tablets, removable media, drives, cameras, smartwatches, and any other device capable of storing digital data in the actual possession or accompanying baggage of the traveller.

#### **Actions required by officers in ICS:**

##### Customs Secondary Referral

- Within the Customs Secondary Referral window, the officer has the ability to record electronic device examinations
- The officer selects the *Open* tab to display the possible secondary actions available
- The officer can select the values *YES* or *NO* for *Electronic Device Search Performed*:
- If the officer selects *YES* to *Electronic Device Search Performed*, then the officer answers *Number of Devices Searched* by entering the number of devices within the box and then selects *NO* or *YES* for *Search Resultant*

**NOTE: only select YES for resultant if the examination of the digital device(s) led to the identification of a contravention of IRPA, the Customs Act and/or any other Act of Parliament**

**Contact Information:**

Traveller Compliance Unit, Program Compliance and Outreach Division, Travellers Branch

Questions regarding this bulletin should be directed to the Traveller Compliance Unit via e-mail at:

**Approved by:** Giovanni Matrisciano, Director  
Program Compliance and Outreach Division  
Traveller Programs Directorate  
Travellers Branch

**Effective Date: 2020-02-30**

**Updated: N/A**



**CANADA BORDER SERVICES AGENCY**  
**POLICY ON PORT OF ENTRY EXAMINATIONS OF TRAVELLERS' DIGITAL DEVICES**

November 2019

<b>POLICY STATEMENT .....</b>	<b>3</b>
<b>DEFINITIONS .....</b>	<b>3</b>
<b>PURPOSE AND SCOPE .....</b>	<b>3</b>
<b>AUTHORITIES – CUSTOMS ACT / IRPA.....</b>	<b>5</b>
<b>ROLES AND RESPONSIBILITIES.....</b>	<b>11</b>
ROLE OF BORDER SERVICES OFFICERS.....	11
ROLE OF INTELLIGENCE OFFICERS .....	11
ROLE OF SUPERINTENDENTS .....	12
ROLE OF CHIEFS .....	12
<b>POLICIES AND PROCEDURES .....</b>	<b>13</b>
WHEN A TRAVELLER’S DIGITAL DEVICE CAN BE EXAMINED.....	13
NOTE TAKING.....	15
WHAT CAN BE EXAMINED .....	17
PRIVACY AND PRESENCE OF TRAVELLER .....	18
DEVICE PASSWORDS AND SECURITY .....	19
DISABLING NETWORK CONNECTIVITY .....	20
HOW A DEVICE SHOULD BE EXAMINED .....	21
COPYING/REPRODUCING DATA FROM A TRAVELLER’S DIGITAL DEVICE .....	22
REPORTING OF DIGITAL DEVICE EXAMINATION.....	23
ENCOUNTERING INTIMATE IMAGES AND OTHER SENSITIVE MATERIAL .....	23
CBSA OFFICERS ENCOUNTERING OFFENSIVE MATERIAL ON DIGITAL DEVICES .....	24
SOLICITOR-CLIENT PRIVILEGED INFORMATION AND JUDICIAL INFORMATION .....	25
ENCOUNTERING EVIDENCE OF A CRIMINAL NATURE .....	26
DIGITAL DEVICE EXAMINATIONS AND LOOKOUT PROCEDURES.....	27
<b>DETENTION AND SEIZURE OF DEVICE.....</b>	<b>28</b>
<b>REFUSAL TO PROVIDE MEANS OF ACCESSING A DIGITAL DEVICE .....</b>	<b>28</b>
<b>SHARING OF INFORMATION OR DATA DISCOVERED ON A TRAVELLER’S DIGITAL DEVICE .....</b>	<b>30</b>
<b>ACCOMPANYING RESOURCES .....</b>	<b>30</b>



## Policy Statement

1. Digital devices, media, documents, software and stored electronic data are considered “goods” under Canada Border Services Agency (CBSA) program legislation and are subject to examination by CBSA Officers at ports of entry/customs offices (hereafter “ports of entry”) for the administration and enforcement of CBSA program legislation. Examinations of digital devices and media can facilitate informed decision-making regarding admissibility and entry of people and goods to Canada under CBSA program legislation. CBSA Officers carrying out examinations of travellers’ digital goods shall adhere to this policy.
2. Though digital devices are considered goods and can be examined as such, as a matter of policy, examinations of digital devices should not be conducted as a matter of course.

## Definitions

3. “Digital device” for the purposes of this policy means mobile phones (cell phones), smartphones, computers, tablets, removable media, drives, cameras, smartwatches, and any other device capable of storing digital data in the actual possession or accompanying baggage of the traveller.
4. If a CBSA Officer is unsure as to whether a digital device is capable of storing digital data the Officer must include the device within the definition of digital device.
5. “CBSA program legislation” is defined in section 2 of the Canada Border Services Agency Act.

## Purpose and Scope

6. The purpose of this policy is to provide CBSA Officers with a framework for the lawful, reasonable and progressive port of entry examinations of travellers’ digital devices while

recognizing and respecting the potential private nature of information contained within these devices<sup>1</sup>.

7. CBSA Officers, as with other non-digital information encountered, are bound to maintain the confidentiality of this information, except where sharing is permitted by law.
8. This policy applies to any CBSA Officer<sup>2</sup> who may, as part of their duties, examine a traveller's digital device as part of a secondary examination under the *Customs Act* or the *Immigration and Refugee Protection Act* (IRPA) at a port of entry.
9. This policy applies to inbound, port of entry examinations of travellers' digital devices.
10. This policy does not apply to commercial quantities of digital devices, or digital devices imported for commercial purposes.
11. This policy does not apply to examinations performed under section 99.3 of the *Customs Act* (see Enforcement Manual Part 6, Chapter 9 – Customs Controlled Areas).
12. This policy does not apply to instances where a traveller's digital device is examined or searched:
  - a. to determine if physical (i.e. non-digital) contraband is contained within or on the device itself (ex: contraband hidden in a cavity within a device);
  - b. under judicial authorization (i.e. search warrant);
  - c. incident to arrest;
  - d. in relation to *IRPA* A16(1) or A16(3), when applied outside of the port of entry context (e.g. overseas or within Canada);
  - e. solely to determine if the digital device functions; or

---

<sup>1</sup> In a criminal investigative inland context, Canadian courts have recognized that digital devices can have unique characteristics that differentiate them from other items subject to a search

<sup>2</sup> The CBSA employee must meet the definition of "officer" under the relevant provisions of the *Customs Act* and the *IRPA* to conduct these examinations under both the *Customs Act* and the *IRPA*

- f. when a traveller displays digital content to an Officer, in an attempt to demonstrate compliance with CBSA program legislation or to provide additional context or information relevant to their admissibility or compliance (ex: a digital copy of a work or study permit, or receipts to show the value of an item), provided the viewing of that content by the Officer does not progress to a more detailed examination of the device's contents not initially displayed to the Officer.

Note: When the above 11. f) circumstances are met, CBSA Officers must still ensure that any subsequent obtaining of information from the interaction is within the scope of lawful authority and is for valid CBSA program legislation purposes.

13. This policy does not limit any examination authority conferred on any CBSA Officer under any Act of Parliament.

#### Authorities – Customs Act / IRPA

14. The *Customs Act* and IRPA authorities to examine digital devices by CBSA Officers at the border can remain available throughout an interaction with a traveller until the examination or assessment is completed. Possible concerns such as identity, admissibility of persons, smuggling and/or release of goods can occur simultaneously.

Note: CBSA Officers must be mindful of distinctions as between CBSA's relevant authorities (eg.: IRPA 16(3) does not apply to Canadian citizens whereas IRPA 139 requires reasonable grounds to believe)."

15. If a digital device examination is performed simultaneously for non-compliance under both the *Customs Act* and the *IRPA*, the examining Officer must adhere simultaneously to the specific legislative criteria under the specific legislative examination authorities on which the

Officer is relying to conduct the digital device examination at the port of entry, as well as this policy.

16. If a digital device examination progresses to require further exercise of CBSA authorities (eg.: obtaining, detaining, seizing, etc.), the relevant officer must continue to adhere to the specific legislative authority's requirements and associated CBSA policy guidance appropriate to the circumstances.

### ***Customs Act – Obligations of Travellers***

17. Section 7.1 of the *Customs Act* states: "Any information provided to an officer in the administration or enforcement of this Act, the *Customs Tariff* or the *Special Import Measures Act* or under any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods, shall be true, accurate and complete."
18. Section 11 (1) of the *Customs Act* states: "every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present [themselves] to an officer and answer truthfully any questions asked by the officer in the performance of [their] duties under this or any other Act of Parliament."
19. Section 12 (1) of the *Customs Act* states: "all goods that are imported shall, except in such circumstances and subject to such conditions as may be prescribed, be reported at the nearest customs office designated for that purpose that is open for business."
20. Section 13 of the *Customs Act* states: "Every person who reports goods under section 12 inside or outside Canada or is stopped by an officer in accordance with section 99.1 shall  
(a) answer truthfully any question asked by an officer with respect to the goods; and

(b) if an officer so requests, present the goods to the officer, remove any covering from the goods, unload any conveyance or open any part of the conveyance, or open or unpack any package or container that the officer wishes to examine.”

### ***Customs Act - Examination of Goods Authorities***

21. Section 99 (1) (a) of the *Customs Act* allows an officer: “at any time up to the time of release, examine any goods that have been imported and open or cause to be opened any package or container of imported goods and take samples of imported goods in reasonable amounts;”
22. Section 99 (1) (e) of the *Customs Act* states: “where the officer suspects on reasonable grounds that this Act or the regulations or any other Act of Parliament administered or enforced by [them] or any regulations thereunder have been or might be contravened in respect of any goods, examine the goods and open or cause to be opened any package or container thereof;”

### ***Customs Act – Detention of Goods Authority***

23. Section 101 of the *Customs Act* states: “goods that have been imported or are about to be exported may be detained by an officer until [they are] satisfied that the goods have been dealt with in accordance with this Act, and any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods, and any regulations made thereunder.”

### ***Customs Act – Seizure of Goods Authority***

24. Section 110 (1) (a) of the *Customs Act* states: “An officer may, where [they believe] on reasonable grounds that this Act or the regulations have been contravened in respect of goods, seize as forfeit

a. The goods;"

25. Section 110 (3) states: "An officer may, where [they believe] on reasonable grounds that this Act or the regulations have been contravened, seize anything that [they believe] on reasonable grounds will afford evidence in respect of the contravention."

***Customs Act – Copying Authority***

26. Section 115(1) states: "If any record is examined or seized under this Act, the Minister, or the officer by whom it is examined or seized, may make or cause to be made one or more copies of it, and a copy purporting to be certified by the Minister or a person authorized by the Minister is admissible in evidence and has the same probative force as the original would have if it had been proved in the ordinary way."

***Criminal Code – Seizure without warrant***

27. Section 489 (2) of the Criminal Code states: "Every peace officer, and every public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, who is lawfully present in a place pursuant to a warrant or otherwise in the execution of duties, may, without a warrant, seize any thing that the officer believes on reasonable grounds

- a. has been obtained by the commission of an offence against this or any other Act of Parliament;
- b. has been used in the commission of an offence against this or any other Act of Parliament; or
- c. will afford evidence in respect of an offence against this or any other Act of Parliament.

***Immigration and Refugee Protection Act (IRPA) – obligations of persons seeking entry***

28. Section 16 (1) of the *IRPA* states: "A person who makes an application must answer truthfully all questions put to them for the purpose of the examination and must produce a visa and all relevant evidence and documents that the officer reasonably requires."
29. Section 16 (1.1) states: "A person who makes an application must, on request of an officer, appear for an examination."
30. Section 16 (2) states: "In the case of a foreign national,
- a. The relevant evidence referred to in subsection (1) includes photographic and fingerprint evidence; and
  - b. Subject to the regulations, the foreign national must submit to a medical examination."
31. Section 18 (1) of *IRPA* states: "Subject to the regulations, every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada."

***Immigration and Refugee Protection Act (IRPA) – examination authorities***

32. Section 15 (1) of the *IRPA* states: "An officer is authorized to proceed with an examination if a person makes an application to the officer in accordance with this Act or if an application is made under subsection 11(1.01)."<sup>3</sup>
33. Section 15 (3) of the *IRPA* states: "An officer may board and inspect any means of transportation bringing persons to Canada, examine any person carried by that means of transportation and any record or document respecting that person, seize and remove the record or document to obtain copies of extracts and hold the means of transportation until the inspection and examination are completed."

---

<sup>3</sup> Section 11 (1.01) of the *IRPA* addresses mandatory electronic travel authorizations made by foreign nationals prior to entry.

34. Section 16 (3) of the *IRPA* states: "An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act."
35. Section 139 of the *IRPA* states: "An officer may search any person seeking to come into Canada and may search their luggage and personal effects and the means of transportation that conveyed the person to Canada if the officer believes on reasonable grounds that the person
- a. has not revealed their identity or has hidden on or about their person documents that are relevant to their admissibility; or
  - b. has committed, or possess documents that may be used in the commission of, an offence referred to in section 117, 118, or 122."

***Immigration and Refugee Protection Act – seizure authority***

36. Section 140 (1) of the *IRPA* states: "An officer may seize and hold any means of transportation, document or other thing if the officer believes on reasonable grounds that it was fraudulently or improperly obtained or used or that the seizure is necessary to prevent its fraudulent or improper use or to carry out the purposes of this Act."

***Immigration and Refugee Protection Act – Copying Authorities***

37. Section 15(3) of the *IRPA* states: "An officer may board and inspect any means of transportation bringing persons to Canada, examine any person carried by that means of transportation and any record or document respecting that person, seize and remove the record or document to obtain copies or extracts and hold the means of transportation until the inspection and examination are completed."



38. Section 16(3) of the IRPA states: “An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act.”

## Roles and Responsibilities

### Role of Border Services Officers

39. BSOs working at ports of entry must be familiar with the policy on the examination of travellers' digital devices.
40. BSOs are responsible for taking the mandatory training on the Examination of Digital Devices
41. BSOs are responsible for adhering to this policy on the examination of travellers' digital devices.
42. As per the policy guidance contained herein, BSOs are responsible for:
- a. remaining sensitive to the potential private nature of data stored on digital devices;
  - b. following guidance on when and how digital devices can be examined;
  - c. reporting any examinations of travellers' digital devices to CBSA Headquarters; and
  - d. making accurate, contemporaneous and detailed notes whenever a traveller's digital device is examined.

### Role of Intelligence Officers

43. Intelligence Officers are responsible for:

- a. Familiarizing themselves with the policy on examinations of travellers' digital devices, and
- b. Remaining available to consult with other CBSA Officers who may examine travellers' digital devices, including BSOs that encounter lookouts when processing travellers, to provide additional information to the BSO that could assist the BSO in determining if a digital device examination is justified.

#### Role of Superintendents

#### 44. Superintendents are responsible for:

- a. Familiarizing themselves with the policy on examinations of travellers' digital devices;
- b. Ensuring BSOs working in the traveller continuum familiarize themselves with the policy on examinations of travellers' digital devices; and
- c. Ensuring BSOs follow the policy guidance contained herein, including but not limited to:
  - i. Not conducting digital device exams as a matter of course;
  - ii. Taking accurate, contemporaneous and detailed notes when devices are examined;
  - iii. Remaining sensitive to the potential private nature of these goods; and
  - iv. Reporting to CBSA HQ all instances of examinations of travellers' digital devices.
- d. Performing periodic compliance verifications to ensure BSOs are following the policies contained herein.

#### Role of Chiefs

45. Chiefs are responsible for:

- a. Ensuring ports of entry in their jurisdiction are aware of the policy on examinations of travellers' digital devices;
- b. Ensuring BSOs in their jurisdiction have completed the requisite training on the examination of digital devices;
- c. Ensuring Superintendents exercise due diligence in reporting instances of digital device examinations to CBSA Headquarters; and
- d. Ensuring Superintendents perform periodic compliance verifications to ensure BSOs are following the policies contained herein, including note taking.

## Policies and Procedures

### When a Traveller's Digital Device Can Be Examined

46. Examinations of travellers' digital devices must be performed with a clear link to administering or enforcing CBSA program legislation that governs the cross-border movement of people and goods, including animals and plants.
47. CBSA officers shall not examine digital devices and media with the sole or primary purpose of looking for evidence of a criminal offence under any Act of Parliament.
48. See the section on Encountering Evidence of a Criminal Nature in this policy for further instruction.
49. An examination of a traveller's digital device should not be conducted as a matter of course.
50. An examination of a traveller's digital device should occur only:

- a. If there is a multiplicity of indicators suggesting evidence of a contravention of CBSA program legislation may be found on the device; or
- b. If concerns exist regarding the traveller's admissibility, identity or non-compliance under the *IRPA* and the Officer is of the view that an examination of the traveller's digital device will provide further information regarding that traveller's admissibility, identity or non-compliance.

## Notetaking

53. Accurate, contemporaneous and detailed record-keeping in officer notebooks is essential when conducting examinations of travellers' digital devices.
54. These note taking requirements must be followed even in the instance that the examination of a traveller's digital device is non-resultant.
55. The note taking directives described herein consider the Supreme Court of Canada jurisprudence in inland contexts in relation to the obligation to keep a careful record when conducting a search of a digital device in the absence either of judicial authorization or reasonable and probable grounds. The note taking directives aim to protect CBSA Officers and support CBSA's legal authorities. Courts have also recognized that the record-keeping requirement will have the incidental effect of helping Officers focus on the question of whether their conduct in relation to the examination of the device falls squarely within the parameters of a lawful examination for CBSA program legislation purposes. In the absence of careful and detailed notetaking, it becomes much more difficult to review the exercise of CBSA authorities and it becomes much more difficult to defend the CBSA against allegations of unlawful conduct.
56. Accurate, contemporaneous and detailed note taking will:
  - a. Assist Officers in being able to articulate each step of a CBSA port of entry digital device examination for the purposes of CBSA program legislation;
  - b. Serve as evidence should legal proceedings ensue;
  - c. Protect the officer and the CBSA should allegations of misconduct arise through internal CBSA complaint mechanisms or external review or complaint bodies;and

- d. Serve as a record of the judicious and lawful use of the statutory authorities available to officers.
57. The note taking directives contained herein are in addition to the note taking requirements identified in the agency's Notebook Policy, found in Part 8, Chapter 1 of the Enforcement Manual.
58. When conducting examinations of travellers' digital devices, Officers should take notes that include, but are not limited to:
- a. indicators observed by the Officer;
  - b. CBSA program legislation rationale for the examination;
  - c. type and description of device;
  - d. password(s), only if the exam was resultant, and any relevant security protection details;
  - e. steps taken to disable network connectivity;
  - f. date and time as it appears on device;
  - g. local date and time;
  - h. duration of the digital device examination;
  - i. areas and items examined on the device (e.g. pictures contained within the gallery application, emails contained within the Gmail application, etc.);
  - j. Rationale for examining each type of data (e.g. one type of data may be digital photos, one type may be documents, etc.) and the nexus to CBSA program legislation (e.g. looking for proof identity in documents);
  - k. the traveller's demeanor and any relevant communication with the traveller with respect to the device and its contents; and

- l. who was involved in the examination of the device and how the examination was performed (e.g. manual examination by one Officer, navigating with smartphone touchscreen).
- m. If examination is resultant, the next steps taken and the associated legislative authorities (e.g. detention, seizure or copying if authorized in the circumstances and required for the administration or enforcement of CBSA program legislation).

### What Can Be Examined

- 59. Any information examined residing on a traveller's digital device must be linked to relevant legislated CBSA program concerns<sup>5</sup> and the examination must take place within the scope of an applicable lawful authority.
- 60. Section 16 (3) of the *IRPA* authorizes an Officer to require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence that may be used to establish their identity or compliance with the *IRPA*. Where an Officer has concerns regarding identity or non-compliance with the *IRPA*, they may examine relevant data on the permanent resident or foreign national's digital device, as reasonably required, to determine identity or non-compliance under the *IRPA*.
- 61. Sections 34 through 42 of the *IRPA* set out the conditions under which a foreign national or permanent resident is inadmissible to Canada. Where an Officer has concerns that an individual may be inadmissible, they may examine relevant data on the traveller's digital device, as reasonably required, to determine admissibility.

---

<sup>5</sup> CBSA program legislation is defined in section 2 of the *Canada Border Service Agency Act*.

62. In terms of importation, under section 99 (1) (a) of the *Customs Act* only goods that have been imported are subject to examination by CBSA Officers, up until the time of release.
63. Therefore, CBSA Officers are only authorized by section 99 (1) (a) of the *Customs Act* to examine data that resides on a digital device at the time of importation, at any time up to the time of release.
64. To avoid mistakenly examining data not residing on the device at the time of importation, officers should take steps to disable network connectivity before the examination begins:  
See the Disabling Network Connectivity section below.

#### Privacy and Presence of Traveller

65. CBSA Officers must remain cognisant of the potential private nature of data stored on travellers' devices, remain sensitive, discreet and professional to minimize potential embarrassment to travellers.
66. Digital devices and media may hold data related to, for example, personal photos, journal entries, text messages, group chats, travel history, intimate imagery, medical information and medical history (see the Encountering intimate images and other sensitive material section), legal advice (see the Solicitor-Client privileged and Judicial information section), financial information, and other private details.
67. Where operationally feasible, Officers should perform examinations of travellers' digital devices in the presence of the traveller to mitigate against potential concerns of the traveller.
68. When a traveller is present for the examination, Officers should be prepared to explain:
- a. the authority under which they are conducting the examination;
  - b. the rationale(s) for the examination, if appropriate; and



- c. that no information will be seized or any data copied unless required as evidence of a contravention or offence.

#### Device Passwords and Security

- 69. Digital devices are frequently protected with a password or other security method (e.g. passcode, biometrics, etc.). In order for an Officer to examine a digital device a traveller must supply the means for the device to be examined.
- 70. Where a password is required to gain access to a digital device, Officers should explain to a traveller that a password must be supplied in order for the traveller's obligations on entry to Canada under the *Customs Act*, the *IRPA* or other CBSA program legislation to be fulfilled.
- 71. While a device may primarily be protected by a biometrics-enabled method, the device can often also be accessed through a password. Where possible, Officers should seek to gain access to devices using this latter type of security method.
- 72. Officers should take great care in inputting the numeric or alphanumeric password. Officers should consider inputting the password a maximum of 2 times, in the event the traveller has enabled a wiping or locking process.
- 73. Officers should notate a device's password on a separate piece of paper in order to ensure it can be accessed at a later date, should prohibited content or evidence be found (see the Note taking directives section for more information).
- 74. If the examination is resultant, Officers should copy the password from the separate piece of paper into their officer notebook.
- 75. If the examination of a digital device is non-resultant, Officers should not retain the password or passcode. Officers should provide the traveller with the piece of paper upon which they recorded the password or passcode. Officers should record that they have done so in their officer notebook.

76. Officers shall inform the traveller that their password or passcode, if retained, will be protected in accordance with privacy legislation.
77. After a non-resultant examination, Officers shall inform the traveller that their password or passcode can be changed immediately.
78. Officers should not record passwords to travellers' digital devices in CBSA systems, including the Integrated Customs Enforcement System (ICES) or the Integrated Customs System (ICS).

Note: Officers should continue to use standard operating procedures to submit passwords to the Prohibited Importations Unit.

#### Disabling Network Connectivity

79. CBSA Officers must only access data that is stored on a traveller's digital device and must not access **any data** stored remotely.
80. In order to prevent accessing remote data, Officers should, before beginning the examination, deactivate its network connectivity.
81. Officers should note the if they were able to deactivate network connectivity in their notebooks.
82. Deactivating network connectivity can also prevent remote wiping or locking.
83. Activating "airplane mode" **may not disable all** network connectivity. Officers must ensure that the device is not connected to a WiFi network, wirelessly tethered to another device, or is sharing a connection with another device via Bluetooth.
84. Normally the status of network connectivity is indicated by icons in the top of the screen. If unsure, an Officer may choose to open the settings of the device and verify connectivity.
85. Officers may also ask the traveller how to disable network connectivity, however, the traveller should not perform this function themselves.

## How a Device Should be Examined

86. Enforcement Manual Part 4, Chapter 3 addresses how Officers should conduct personal baggage, goods and conveyance examinations. This policy on port of entry examinations of travellers' digital devices offers further precision in respect of examining travellers' digital goods but should be read in conjunction with that chapter of the manual.
87. Enforcement Manual Part 4, Chapter 3 stipulates that all examinations by Officers must be conducted in strict adherence to the CBSA's core values. Examinations must be proficient and discrete to the extent possible with respect to travellers and their goods, and all examinations must be conducted in a courteous and professional manner in accordance with the CBSA Code of Conduct.
88. Just as secondary examinations should be methodical, progressive and responsive as new indicators or information is discovered by or revealed to the Officer, so should any secondary examination of a traveller's digital device.
89. An examination of a traveller's digital device should be tailored to the purposes of the CBSA program legislation and should not be conducted as a matter of course.
90. In order to expedite the examination and if practical, an Officer may ask the traveller to point to the relevant area of the device for which the Officer has CBSA border screening and processing concerns. Focussing the examination will maximize efficiency for the Officer and minimize inconvenience to the traveller.
91. As a matter of policy, a port of entry digital device examination should be limited to:
- a. the examination of content for concerns related to CBSA program legislation; and
  - b. areas of the device and data directly related to indicators or concerns identified by the Officer during the interaction with the traveller.

92. Officers should be able to clearly articulate their reasoning for examining each type of data on the device, its link to indicators or concerns identified by the Officer, and the data's anticipated relevance to CBSA program legislation.
93. If, during the examination, additional indicators of concern are observed, the examination may expand and progress beyond the Officer's initial intent, provided diligent notes are taken regarding how and why the examination progresses.
94. Port of entry examinations should only be conducted manually and without the assistance of software/hardware.

#### Copying/Reproducing Data From a Traveller's Digital Device

95. Officers shall advise the traveller that their information will be protected by CBSA in accordance with applicable law including the *Privacy Act* and the *Customs Act*.
96. Officers shall not make copies of, duplicate or reproduce data examined on digital devices, including taking photographs or screenshots, unless such copying is authorized in the circumstances under CBSA program legislation and required for the specific and direct administration or enforcement of CBSA program legislation.
97. Officers shall not notate in their notebook or record in a CBSA system personal any information including contacts, phone numbers, names, dates of birth or other information from devices unless such notating or recording is authorized in the circumstances under CBSA program legislation, and required for the specific and direct administration or enforcement of CBSA program legislation.
98. Officers may rely on their regulatory copying authorities appropriate to the circumstances (*Customs Act* 115(1), IRPA 15(3) or 16(3)) if the legislative criteria in the relevant authority are met, and, only if the copying is for the specific and direct regulatory administration or enforcement of CBSA program legislation. In these cases, travellers are to be informed that

their information has been copied and that their information will be protected by the CBSA in accordance with applicable law including the *Privacy Act* and *Customs Act*.

99. Officers must use a CBSA-issued camera for any copying and must note the timestamp on the photograph in their notebook.
100. Officers must be cognizant of where the regulatory examination crosses over to the realm of criminal investigation. Following the lawful initiation and progression of a digital device examination for CBSA program legislation purposes, in cases where evidence of a criminal offence is uncovered and Officers need to copy already lawfully examined information, Officers must first seize the device under legislative seizure authorities appropriate to the circumstances.

#### Reporting of Digital Device Examination

101. Effective November 2017, all examinations of travellers' digital devices must be reported to CBSA Headquarters as per Operational Bulletin 2017-61.
102. It is the policy of the CBSA to nationally track:
  - a. the number of examinations of travellers' digital devices;
  - b. the date of the examinations; and
  - c. the port of entry at which the examinations took place.
103. CBSA Officers are expected to record in their notebooks all other information pertaining to digital device exams as per the Note taking directives section (e.g. the indicators that led to the digital device examination, the areas of the device accessed, etc.).

#### Encountering Intimate Images and Other Sensitive Material

104. A traveller may be particularly concerned if intimate images<sup>6</sup> of themselves or others are saved on the device.
105. If a traveller alerts an Officer to the presence of intimate images of themselves or others, the Officer should ask the traveller if there is a way to reasonably circumvent the viewing of those images.
106. If it is likely that exposure to the intimate images is unavoidable, Officers should ask the traveller whether they would be more comfortable if an Officer of another sex temporarily assists in viewing the digital device's content, until such point where exposure to the intimate images could no longer be a concern (e.g.: an assisting Officer peruses a photo gallery to confirm that prohibited content is not saved in that location, then returns the device to the primary examining Officer).
107. Provided that circumventing the data does not impede the Officer's exercise of CBSA program legislation authorities and responsibilities in carrying out the examination, Officers should consider the same procedure as described in paragraph 105 should a traveller alert an officer to content related to: banking/financial information, corporate/trade secrets, intellectual property, medical information, solicitor-client privileged information, judicial information or a journalist's work-related information.

#### CBSA Officers Encountering Offensive Material on Digital Devices

108. During the course of an examination of a traveller's digital device, a CBSA Officer may encounter material that may be offensive or upsetting.
109. The Intervention Protocol – Exposure to Offensive Material was established to mitigate against the potential negative effects of exposure to offensive material, to create a

---

<sup>6</sup> Intimate image is defined in s. 162.1 (2) of the *Criminal Code*.

framework for management intervention and to make employees aware of the support resources available to them should they be affected by exposure.

110. It is recommended that CBSA Officers who could be exposed to offensive material should also take the online course, *Mitigating the Impacts of Exposure to offensive materials, horrific images, and traumatic events* (course code H2049-P).

#### Solicitor-Client privileged information and Judicial information

111. For more information regarding CBSA's solicitor-client privilege policy, consult Enforcement Manual Part 4 Chapter 3.
112. Solicitor-client privilege applies to any record of confidential communication between lawyers and clients where legal advice or assistance was sought, provided or otherwise involved. The privilege includes information gathered to formulate legal advice, such as lawyer's working documents, memos and files. Solicitor-client privilege belongs to clients. Lawyers carrying these communications are duty-bound to protect confidentiality and must assert this privilege on their client's behalf.
113. Judicial information is information carried by a judge and that needs to remain confidential in order to protect and preserve judicial independence.
114. CBSA Officers should not examine content clearly marked as being subject to solicitor-client privilege, nor should they examine content that a traveller asserts privilege over. Officers should also not examine content if, over the course of an examination, the Officer becomes aware of potential solicitor-client privilege.
115. In the context of an examination of a digital device, it may be more difficult to determine what is and what is not subject to this privilege.

116. If a traveller asserts solicitor-client privilege over data saved on a digital device or claims such data to be judicial information, an Officer should ask that the traveller record in writing the locations in which such data is saved.
117. Officers should explain to the traveller the process involved in confirming solicitor-client privilege or judicial information as per the guidance below.
118. If an Officer can proceed with the digital device exam and avoid exposure to the data over which privilege is asserted, the Officer should proceed with due care.
119. If an Officer believes that the examination would compromise the solicitor-client privilege or judicial information, the Officer should:
- a. Notify and consult with their immediate supervisor with respect to the circumstances; and
  - b. Determine with the supervisor if the device should be released, or
  - c. Detain (*Customs Act* 101) or seize (*IRPA* 140(1)) the device without being examined, seal the device in a package marked with the assumption they are privileged, and set the device aside for review by a court or analogous independent review body for confirmation of privilege.
120. Officers can contact their region's Justice Liaison Officer for information on how to proceed with confirmation of privilege.
121. If the traveller refuses to grant access to their device, the Officer should explain that their device is being detained/seized and will be sealed and set aside for independent review to confirm privilege. If the traveller continues to refuse access, the Officer should follow the guidelines in the Refusal to Provide Access section of this policy.

#### Encountering Evidence of a Criminal Nature



122. Where evidence of a criminal offence is discovered during the examination process, officers must be cognisant of where the regulatory examination crosses over to the realm of a criminal investigation. Officers must determine on a case-by-case basis, through consultation with their supervisor, whether or not to continue the regulatory examination and identify any possible impacts on potential criminal investigations.
123. Officers must be prepared to articulate the ongoing *Customs Act* or *IRPA* purpose of the exam and the authority under which they are operating and be cautious to ensure that the exam is not continuing for the sole or primary purpose of discovering evidence of a criminal offence.
124. In situations where evidence discovered during the *Customs Act* or *IRPA* examination appears to merit a criminal investigation, the examination should cease and the device secured and seized under the appropriate authority to permit the investigating agency (e.g. CBSA Criminal Investigations or the police of jurisdiction) to seek a warrant to forensically extract, analyze and preserve the digital evidence, as required.
125. In these circumstances, officers must also be cognisant that continuing the examination could potentially alter digital evidence (e.g. timestamps indicating when the file was last accessed).

#### Digital Device Examinations and Lookout Procedures

126. The CBSA Lookout Policy and CBSA Lookout Standard Operating Procedures are the primary guidance documents related to encountering and issuance of lookouts.
127. Officers must use their discretion when deciding if a digital device examination of a traveller subject to a lookout is justified, based on the information in the lookout and the information available to them at the port of entry during processing of the traveller.

128. For further clarity, in the event a lookout advises an Officer to conduct an examination of a traveller's digital device at secondary, the Officer is still responsible for the reasonable exercise of their authority, including secondary examination progression and is still required to adhere to this policy. The responsible Officer can contact the lookout issuer to gather further information for consideration appropriate to the circumstances.

#### Detention and seizure of device

129. Part 5, Chapters 2 and 3 of the Enforcement Manual are the primary guidance documents for the seizure of evidence and goods from travellers.

#### Refusal to provide means of accessing a digital device

130. During a border examination upon entry to Canada, travellers have the legal obligation under the *Customs Act* to provide the means to access their goods, including digital devices, as well as the obligation to produce all relevant evidence that an Officer reasonably requires under the *IRPA*.

131. Every reasonable opportunity should be given to the traveller to fulfill their obligations at the port of entry under CBSA program legislation in providing the means to access their digital device.

132. In circumstances where a traveller refuses to provide the means to access their digital device, and where such refusal does not result in denial of entry under *IRPA*, provided the relevant legislative authority criteria are met, the device may be:

- a. Detained under section 101 of the *Customs Act*; or
- b. Seized and held under subsection 140 (1) of the *IRPA*; and
- c. Assistance from a CBSA expert may be obtained.

However, per the Digital Forensic Investigations Policy, prior to Digital Forensic Investigators providing assistance with examinations falling outside the scope of Criminal Investigations' and Enforcement and Intelligence priorities, senior management approval must be obtained and the examination may only be conducted when legislative and regulatory authorities permit.

Note: Officers should also note that the Prohibited Importations Unit (PIU) does not provide digital forensic support. The role of the PIU is to perform tariff classifications for suspect materials (obscenity, hate propaganda, child pornography, etc.). Officers should provide the password(s) to the device(s) and point to suspect images and/or documents within the device(s) when forwarding goods to the PIU for determination.

133. During the course of a regulatory examination of a traveller's digital device at secondary, assistance to gain access to the device shall not be obtained from any source outside the CBSA.
134. Under the *Customs Act*, as a matter of policy, Officers should consider detention first in cases where travellers refuse to provide access to their device rather than seizure.
135. A traveller's digital device cannot be detained in perpetuity, therefore the following timeframes must be observed for detentions under section 101 of the *Customs Act*:
  - a. In the event a traveller's digital device needs to be detained under the *Customs Act* for more than 30 calendar days, approval must be obtained by the Chief of the port of entry each 30 calendar days after the initial 30 days, until a maximum of 90 calendar days of detention is reached; and
  - b. After a maximum 90 days of detention, the device must either be released back to the traveller or seized, in accordance with the applicable legislative seizure authority, requirements and associated CBSA policy guidance.
136. A traveller's digital device can be seized as forfeit under the authority of section 110(1) of the *Customs Act*, provided the Officer believes on reasonable grounds that the *Customs Act* or regulations have been contravened with respect to the goods.
137. Where a traveller has refused to provide the means to access their digital device:

- a. the device can be seized under section 110 of the *Customs Act* on the basis that the traveller contravened section 13 of the *Customs Act*, or
  - b. the device can be seized under subsection 140 (1) of the IRPA on the basis doing so is necessary to carry out the purposes of the Act.
138. CBSA officers shall not arrest a traveller for hindering (Section 153.1 of the *Customs Act*) or for obstruction (paragraph 129(1)(d) of IRPA) solely for refusing to provide a password.

#### Sharing of information or data discovered on a traveller's digital device

139. The CBSA's primary guidance document on disclosure of "customs information," as defined in Section 107 of the *Customs Act*, is the Policy on the Disclosure of Customs Information: Section 107 of the Customs Act. This document should guide CBSA Officers when determining if they may provide access to customs information, in any form (e.g. hard copy, electronic or video format).
140. If information collected during a secondary examination does not meet the definition of "customs information" but instead meets the definition of "personal information" as defined in the *Privacy Act*, CBSA Officers should consult the Policy on the Disclosure of Personal Information: Section 8 of the Privacy Act for guidance.

#### Accompanying Resources

141. This policy document is not intended to be a standalone document, and should be read in conjunction with the following resources:
- Canada Border Services Agency Act
  - Customs Act
  - Immigration and Refugee Protection Act
  - Privacy Act
  - Criminal Code
  - Canada Border Services Agency Code of Conduct
  - Canada Border Services Agency Enforcement Manual

Enforcement Manual  
Operational Bulletins  
Shift Briefing Bulletins  
Training and Learning products

Please note: This is not an exhaustive list of resources; the list will be updated as policy changes are made.